



## The *Comm*Law Group

HELEIN & MARASHLIAN, LLC  
1483 Chain Bridge Road  
Suite 301  
McLean, Virginia 22101

Telephone: (703) 714-1300  
Facsimile: (703) 714-1330  
E-mail: [mail@CommLawGroup.com](mailto:mail@CommLawGroup.com)  
Website: [www.CommLawGroup.com](http://www.CommLawGroup.com)

Writer's Direct Dial Number  
703-714-1313

Writer's E-mail Address  
[jsm@commlawgroup.com](mailto:jsm@commlawgroup.com)

September 11, 2008

*ELECTRONICALLY FILED*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street SW  
Washington, D.C. 20554

**Re:    *Filed in EB Docket No. 06-36***  
***Certification of CPNI Filing September 11, 2008***

Dear Secretary Dortch:

On behalf of WERCS Communications, Inc. its attorneys hereby file its Certification of Compliance with Section 222 of the Communications Act and Commission Rules implementing Section 222.

An additional copy of this filing is also enclosed, to be date-stamped and returned in the envelope provided.

Should there be any questions regarding this filing, kindly contact the undersigned.

Respectfully submitted,

/s/

Jonathan S. Marashlian

Enclosure

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008**

**Date Filed:** September 11, 2008

**Name of Company**  
**Covered by this Certification:** WERCS Communications, Inc.

**Form 499 Filer ID:** 826312

**Name of Signatory:** James Moberly

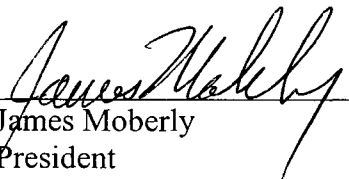
**Title of Signatory:** President

I, James Moberly, certify that I am President of WERCS Communications, Inc. ("WERCS"). I attest that, as an officer of WERCS, I am authorized to execute this CPNI Compliance Certification on the company's behalf.

I have personal knowledge that WERCS' business methods and the procedures adopted and employed by WERCS are adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996 ("the Act"), and the Federal Communications Commission's regulations implementing Section 222 of the Act, 47 C.F.R. § 64.2005, 64.2007 and 64.2009.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year. The company has no information to report with respect to the processes pretexters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed:   
James Moberly  
President

**Accompanying Statement to  
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008**

To the extent WERCS receives or obtains access to CPNI, it has implemented the following practices and procedures with respect to the use, marketing, and disclosure of such CPNI:

Employee Training and Discipline

- Train all employees and personnel as to when they are and are not authorized to use CPNI.
- Institute an express disciplinary process for unauthorized use of CPNI.

Sales and Marketing Campaign Approval

- Guarantee that all sales and marketing campaigns are approved by management.

Record-Keeping Requirements

- Establish a system to maintain a record of all sales and marketing campaigns that use their customers' CPNI, including marketing campaigns of affiliates and independent contractors.
- Ensure that these records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- Make certain that these records are maintained for a minimum of one (1) year.

Establishment of a Supervisory Review Process

- Establish a supervisory review process for all outbound marketing situations.
- Certify that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval.

Opt-In

- Guarantee that the Company only discloses CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties only after receiving “opt-in” approval from a customer.
- Verify that the Company enters into confidential agreements with joint venture partners, independent contractors or any other third party when releasing CPNI.

Opt-Out Mechanism Failure

- Establish a protocol through which the Company will provide the FCC with written notice within five (5) business days of any instance where opt-out mechanisms do not

work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

#### Compliance Certificates

- Execute a statement, signed by an officer, certifying that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI regulations.
- Execute a statement detailing how operating procedures ensure compliance with CPNI regulations.
- Execute a summary of all customer complaints received in the past year concerning unauthorized release of CPNI.

#### Customer Authentication Methods

- Institute customer authentication methods to ensure adequate protection of customers' CPNI. These protections only allow CPNI disclosure in accordance with the following methods:
  - Disclosure of CPNI information in response to a customer providing a pre-established password;
  - Disclosure of requested CPNI to the customer's address or phone number of record; and
  - Access to CPNI if a customer presents a valid photo ID at the carrier's retail location.

#### Customer Notification of CPNI Changes

- Establish a system under which a customer is notified of any change to CPNI. This system, at minimum, notifies a customer of CPNI access in the following circumstances:
  - password modification,
  - a response to a carrier-designed back-up means of authentication,
  - online account changes, or
  - address of record change or creation.

#### Notification to Law Enforcement and Customers of Unauthorized Access

- Establish a protocol under which the appropriate Law Enforcement Agency ("LEA") is notified of any unauthorized access to a customer's CPNI.
- Ensure that all records of any discovered CPNI breaches are kept for a minimum of two (2) years.